

BWB:GKS
F. #2015R01255

15M 1125

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - X

UNITED STATES OF AMERICA

- against -

MOHAMMAD CHOWDHURY,
FAROOQ AHMAD,
JAMSHED BABAR,
UZMA BABAR,
JASON WALKER and
AHMED SOYBAL,
also known as "Ali Aloub,"

Defendants.

- - - - - X

EASTERN DISTRICT OF NEW YORK, SS:

WILLIAM DUFFIN, being duly sworn, deposes and states that he is a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), and the El Dorado Financial Crimes Task Force, duly appointed according to law and acting as such.

On or and about and between 2012 and 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants MOHAMMAD CHOWDHURY, FAROOQ AHMAD, JAMSHED BABAR, UZMA BABAR, JASON WALKER and AHMED SOYBAL, also known as "Ali Aloub," (collectively, "DEFENDANTS"), did knowingly and willfully conspire with intent to defraud and effect transactions with one or more counterfeit or unauthorized access devices, in a manner affecting interstate commerce, and to receive payment or any thing of value during any one year period,

TO BE FILED UNDER SEAL

**AFFIDAVIT AND
COMPLAINT IN SUPPORT OF
APPLICATION FOR ARREST
WARRANT**

(18 U.S.C. § 1029(b)(2))

the aggregated value of which is equal to or greater than \$1,000, in violation of Title 18, United States Code, Sections 1029(a)(2) and 1029(a)(5).

(Title 18, United States Code, Section 1029(b)(2))

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with HSI. I am currently assigned to the El Dorado Task Force ("Task Force"), a multi-agency federal and state task force investigating financial crimes. My duties include conducting and assisting in investigations into various financial frauds including money laundering and identity theft. I have participated in numerous investigations involving financial frauds, during the course of which I have interviewed suspects and witnesses, executed court-authorized search and arrest warrants and used other investigative techniques to secure relevant information, including the examination of computers and other electronic devices. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to carry out their activities. I am familiar with the facts and circumstances set forth below from my participation in the investigation, discussions with other law enforcement officials, my review of documents and my training and experience. Statements attributable to individuals herein are set forth in sum and substance.

¹ Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

BACKGROUND

2. During the course of my work as an agent, I have been involved in investigations of what are commonly referred to as check-kiting schemes, credit card bust-out schemes and synthetic identity fraud schemes.

3. In a check-kiting scheme, an individual typically opens one or more checking accounts (also known as demand deposit accounts) and/or line of credit accounts at a bank. Account holders typically deposit fraudulent checks or checks drawn on accounts with insufficient funds into the checking account and then withdraw the funds in cash transactions at Automated Teller Machines ("ATMs") or at bank teller windows before the bank discovers that the these checks do not clear. These individuals exploit the lag time between a bank receiving a fraudulent check deposit, and shortly thereafter making funds available for use, and the bank subsequently discovering that the deposited check is fraudulent. Where an account holder also opens a line of credit account at the same bank, the account holder typically advances funds from the line of credit account to the checking account and then withdraws the funds shortly thereafter from the checking account in cash transactions at ATMs and bank teller windows. The account holder typically uses fraudulent checks or checks drawn on accounts with insufficient funds to repay the balance on the line of credit account. These checks are returned, resulting in a loss to the bank in the amount extended to the account holder through the line of credit account.

4. In a credit card bust-out scheme, credit card holders typically take their charge cards to collusive merchants who make fraudulent charges on these cards. These fraudulent charges include, but are not limited to, charges that purport to be for merchandise or services, but for which no actual merchandise or services are exchanged, and charges for which

the collusive merchants and credit card holders know the card issuer will never be paid.

Frequently, the credit card holder is paid a fee by the collusive merchant, often a percentage of the value of the fraudulent charges, for the fraudulent use of the credit cards. The credit card holder who allows these fraudulent charges has no intention of paying the credit card issuer for these charges. Frequently, the credit card holder makes fraudulent payments to the credit card issuer using fraudulent checks or checks drawn on accounts with insufficient funds. Upon receipt of these fraudulent payments, but before determining whether the payments will clear, credit card issuers frequently apply these payments to the available balance of the credit card, essentially inflating the available credit limit on the charge card by the amount of the fraudulent payment. The credit card holder and collusive merchant will then make additional fraudulent charges on the charge card until either the additional credit generated from the fraudulent payments is consumed or the credit card issuer learns that there are insufficient funds to cover the fraudulent payment. When the credit card debt goes unpaid, credit card companies first categorize it as 30, 60 or 120 days delinquent. After the debt has been overdue for 120 days, the issuer moves it into the "collections" category. If the collection effort is unsuccessful, the issuer moves the debt into the "write-off" category and typically incurs a loss.

5. In a synthetic identity fraud scheme, the perpetrators of the scheme will typically open bank and credit card accounts in the names of one or more other individuals. The putative account holders are not real people. Rather, the perpetrators combine various pieces of personal identifier information (e.g., names, dates of birth, addresses and Social Security numbers) from different individuals, either real or fictitious, to create a fictitious synthetic identity that appears, for all intents and purposes, to represent a real person but, in reality, does not. The perpetrators typically open various types of accounts at different

financial institutions for a given synthetic identity using the same synthetically-combined personal identifier information. Possession and use of a stable of synthetic identities frequently permits fraud perpetrators to commit a substantial number of check-kiting, line of credit or credit card bust-out frauds.

6. In addition to direct fraudulent transactions with financial institutions, perpetrators of check-kiting, line of credit fraud, credit card bust-out schemes and synthetic identity fraud frequently create and/or control shell companies (which have little or no legitimate business purpose) from which seemingly legitimate purchases of goods or services are made or to which charges from fraudulent credit or debit cards are sent. Shell companies are also frequently used to write checks to artificially inflate the credit limit for a credit card account, make fraudulent deposits into checking accounts, or make fraudulent repayments on line of credit accounts. Investigators frequently discover that a company is a shell company with no legitimate business purpose through a number of methods. For example, investigators may determine that the address purportedly used to conduct business is either fictitious or that there is no apparent business activity being transacted there that matches the ostensible business purpose of the firm. A review of bank accounts and other financial statements for the company may reveal that there are no apparent legitimate business income or business expenses, such as payroll, expenses or cost of goods. Additionally, investigators may identify fraudulent bank and credit card accounts used for check-kiting, line of credit fraud or credit card bust-outs and discover from financial records that a company with no apparent legitimate business purpose is receiving a high volume of transactions—including debit card and credit card transactions—from these fraudulent accounts, indicating that one of the primary purposes of the company is to facilitate the use of such fraudulent accounts.

SUMMARY

7. As set forth below, the defendants' conspiracy involved check-kiting, line of credit fraud, credit card bust-outs and synthetic identity fraud. In particular, the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD controlled over 20 synthetic identities that held checking accounts, line of credit accounts, and credit cards. CHOWDHURY and AHMAD used these synthetic identities to, among other things, make various fraudulent deposits into the checking accounts and withdraw the funds in ATM and teller transactions before the bank discovered that the deposits were fraudulent. CHOWDHURY's and AHMAD's check-kiting and line of credit frauds have resulted in over \$290,000 in losses to financial institutions. CHOWDHURY and AHMAD further made fraudulent purchases using credit cards in the names of various synthetic identities. Their credit card fraud activity is believed to have caused over \$1 million in losses to financial institutions.

8. CHOWDHURY and AHMAD are also believed to control numerous shell companies with little or no business purpose, but which are believed to have used or possessed equipment that enabled them to accept purchases from fraudulent credit cards controlled by CHOWDHURY and AHMAD. From approximately 2012 to 2013, the defendants JASON WALKER and AHMED SOYBAL served as middlemen or salesmen who worked with a number of these shell companies to submit applications to credit processing firms and credit card equipment firms to gain the ability to accept credit card purchases. A company controlled by WALKER also accepted over \$22,000 in fraudulent credit card purchases from cards in the names of synthetic identities controlled by CHOWDHURY and AHMAD. ~~WALKER and SOYBAL served as~~ *JD*

9. The defendants MOHAMMAD CHOWDHURY and FAROOQ

AHMAD also used credit cards in the names of various synthetic identities to make hundreds of fraudulent purchases with collusive merchants, including Isha Grocery, a business owned and operated by the defendants JAMSHED BABAR and UZMA BABAR.² Between approximately 2012 and 2015, Isha Grocery accepted hundreds of transactions totaling over \$680,000 from fraudulent credit cards, including over \$300,000 from fraudulent credit cards controlled by CHOWDHURY and AHMAD.

MOHAMMAD CHOWDHURY AND FAROOQ AHMAD'S FRAUDULENT ACTIVITY

10. Based on a review of credit card documents, investigators identified three credit cards that were applied for by three individuals ("Fairuz Chatterjee," "Farhunz Chowdry," and "Mark Sydney") who each provided an address of 114-06 Linden Blvd. in South Ozone Park, New York. Charges were made on these cards over a short period of time to companies that were later identified to be shell companies with no legitimate business purpose, including one shell company named Didarul Home Improvement, based on a lack of apparent business activity at their physical locations and financial records revealing little or no business activity other than transactions with fraudulent accounts. As described further below, Didarul Home Improvement and other shell companies were used repeatedly by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD to receive fraudulent credit card payments and further the check-kiting and line of credit schemes. The credit card balances for the three credit cards were not paid, resulting in a loss to the credit card issuers.

² Two other collusive merchants, co-conspirators ASAD NAZIR and TAHIRA NAZIR, were arrested and arraigned on Friday, November 20, 2015 before the Hon. Robert M. Levy, United States Magistrate Judge. United States v. Asad (15-MJ-1113).

11. Contact by investigators with the owner of 114-06 Linden Blvd. in South Ozone Park, New York revealed that the three individuals whose names appeared on the credit cards were not associated with that address. A further review of documents and databases revealed that the names appeared to be the result of synthetic identity theft. For example, the personal identifying information used to open the accounts of “Fairuz Chatterjee,” “Farhunz Chowdry,” and “Mark Sydney” did not correspond to a real person. Further investigation revealed that the same names and addresses for these three individuals were used in other financial frauds, in particular a line of credit fraud scheme and a check-kiting scheme, resulting in substantial financial losses.

12. As described in further detail below, using evidence of surveillance photographs, addresses, Internet Protocol (“IP”) addresses, bank accounts, fraudulent purchases made at collusive merchants, and fraudulent purchases made through shell companies, the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD were identified as participants in related credit card fraud, line of credit and check-kiting schemes.

I. USE OF SYNTHETIC IDENTITIES

13. Both the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD used synthetic identities while participating in their fraudulent schemes. The following examples illustrate the operation of the fraudulent schemes using two of the synthetic identities, “Farhunz Chowdry” and “Abigail Singh.”³ CHOWDHURY and AHMAD, however, used over 20 synthetic identities to participate in their fraudulent schemes.

³ These specific examples of synthetic identities, like the others included in this Complaint, are merely illustrative and do not fully describe the scope or extent of the fraud uncovered by the investigation thus far.

A. “Farhunz Chowdry”

14. “Farhunz Chowdry” is a fictitious synthetic identity that was created for the purpose of carrying out the fraudulent scheme. The defendants MOHAMMAD CHOWDHURY and/or FAROOQ AHMAD created this identity using various pieces of personal identifier information. Although “Farhunz Chowdry” possesses a date of birth, Social Security number, and other personal identifier information typically required to open a credit card and/or bank account, he or she is not a real person.

15. “Farhunz Chowdry” opened a line of credit account and checking account at Santander Bank in 2012. Between approximately December 19, 2012 and February 12, 2013, nine advances were made from the line of credit account to the checking account totaling approximately \$11,500. One card purchase was made at the aforementioned Didarul Home Improvement, a shell company with no legitimate business purpose or activity, for approximately \$2,495 on or about February 19, 2013.⁴ Between approximately December 21, 2012 and February 15, 2013, over 40 cash withdrawals were made from the checking account of “Farhunz Chowdry.” On approximately seven dates in that time span, “Farhunz Chowdry” made multiple withdrawals of \$500 each on the same date from different Santander Bank branches in Brooklyn and Queens, New York. On or about February 4, 2013, for example, “Farhunz Chowdry” made three withdrawals of \$500 each from Santander Bank branches in Bayside, Howard Beach, and Jackson Heights, New York. Payments made to the line of credit

⁴ As discussed in further detail below, shell companies are frequently able to obtain equipment used for processing credit card transactions such as countertop credit card swiping machines and pinpad devices. Shell companies also frequently obtain bank accounts into which credit card processors or issuers deposit the proceeds of credit card transactions that are later determined to be fraudulent.

account to repay the aforementioned advances were all reversed with the exception of one \$25 payment. The fraudulent payments included several checks from fraudulent or fictitious accounts at the First National Bank of Omaha.

16. “Farhunz Chowdry” also possessed a credit card account at FIA Card Services in January 2013 and, in that month, made approximately \$14,612 in charges at, among others, the aforementioned shell company Didarul Home Improvement. Approximately \$9,787 in payments was made; all were reversed and resulted in losses to the financial institution.

17. Further investigation revealed additional fraudulent accounts opened using various synthetic identities and identified the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD as the individuals controlling the synthetic identities. Almost 20 accounts, including that associated with “Farhunz Chowdhury,” were opened at Santander Bank. Investigators contacted Santander Bank in 2013 to obtain transaction records, photographs from ATMs and other surveillance footage. Surveillance photographs revealed two males in their early to mid-30s who were conducting transactions on the fraudulent accounts. The transaction records from Santander Bank revealed a number of mailing addresses that were used repeatedly for accounts opened by various synthetic identities, including one located at 85-15 Kendrick Place, Jamaica, New York 11432 (“85-15 Kendrick Place”). Using commercial databases, investigators determined the identity of the residents of 85-15 Kendrick Place, including a male in the same age range as one of the males captured in the surveillance photographs. Investigators obtained records from the New York State Department of Motor Vehicles (“DMV”) for this individual’s driver’s license and associated photographs. The DMV records showed the male living at 85-15 Kendrick Place to be the

defendant MOHAMMAD CHOWDHURY.

18. Investigators compared the surveillance photographs obtained from Santander Bank with the photographs obtained from the DMV and determined that the defendant MOHAMMAD CHOWDHURY was one of the two males conducting transactions on the fraudulent accounts at Santander Bank. Investigators also obtained photographs of CHOWDHURY conducting transactions on an account in his own name at Chase Bank to further confirm the identification. As described above, “Farhunz Chowdry” made three withdrawals of \$500 each from a Santander Bank account on February 4, 2013 at bank branches in Bayside, Howard Beach, and Jackson Heights, New York. ATM surveillance photos captured CHOWDHURY conducting the transactions on that date at the Bayside and Howard Beach, New York bank branches.

19. Investigators subsequently conducted surveillance outside the defendant MOHAMMAD CHOWDHURY’s residence at 85-15 Kendrick Place and observed an unknown male in a white Lexus in close proximity to the home. Investigators recorded the license plate number and obtained both registration information and a photograph from the DMV. This individual was identified as the defendant FAROOQ AHMAD. A comparison of Santander Bank ATM surveillance footage and the DMV photograph revealed that AHMAD was the other unknown male conducting transactions on the fraudulent Santander Bank accounts, including those of “Farhunz Chowdry.”

B. “Abigail Singh”

20. “Abigail Singh” is another synthetic identity created for the purpose of carrying out fraudulent schemes. Like “Farhunz Chowdry,” “Abigail Singh” possesses

personal identifying information, but investigators have determined that this information does not correspond to a real person.

21. “Abigail Singh” opened a checking account at Santander Bank in early 2012. Surveillance photos from Santander Bank ATMs captured the defendant FAROOQ AHMAD conducting transactions on the account on or about, among other dates, January 8, 2014 and January 15, 2014. In mid-2014, “Abigail Singh” opened a Santander Bank credit card account using the same personal identifying information as for the Santander Bank checking account. In July 2014, three checks totaling approximately \$14,600 from a First National Bank of Omaha account purportedly in the name of “Abigail Singh” were mailed to Santander Bank. Santander Bank accepted these payments and applied them to increase the credit limit of the credit card. Before Santander Bank discovered that these checks were fraudulent, “Abigail Singh” made substantial purchases with the credit card, resulting in a loss to Santander Bank of approximately \$19,714.

22. In addition to their both conducting transactions on the same fraudulent accounts and investigators’ observations of the defendant FAROOQ AHMAD’s presence near the defendant MOHAMMAD CHOWDHURY’s home, investigators have obtained EZ-Pass account records from MTA Bridges & Tunnels showing one of AHMAD’s Lexus vehicles, bearing New York license plate number GPX5950, listed as an authorized vehicle on CHOWDHURY’s personal EZ-Pass account as of August 2015. The EZ-Pass records indicate that this vehicle has been listed on CHOWDHURY’s account since June 2014.

II. FINANCING OF 85-15 KENDRICK PLACE

23. The Task Force has further uncovered evidence that the defendant MOHAMMAD CHOWDHURY has used the funds gleaned from these fraudulent schemes to, among other things, finance 85-15 Kendrick Place.

24. Investigators have determined that the home located at 85-15 Kendrick Place is owned in name by the defendant MOHAMMAD CHOWDHURY's in-laws. A Sovereign Bank checking account was opened in December 2007 in the name of "Rupok Bhowmik." Bank records reveal that the personal identifying information provided to open the account of "Rupok Bhowmik" is from yet another synthetic identity because the associated personal identifying information corresponds with a real person. Furthermore, a credit card processing application submitted for the aforementioned shell company, Didarul Home Improvement, to Cynergy Data, a credit card processor, attached a voided check containing the same account information as that of "Rupok Bhowmik," but with "Rupok Bhowmik's" name erased and replaced with "Didarul Home Improvement." In my training and experience, fraud perpetrators frequently submit the same or substantially similar document, such as a voided check, with the name or address altered on different applications at various financial institutions.

25. The bank account of "Rupok Bhowmik" received certain of the proceeds of the credit card fraud. ATM surveillance photographs show the defendant MOHAMMAD CHOWDHURY conducting transactions on the Sovereign Bank account of "Rupok Bhowmik" in 2013. Further, in 2008, checks were written from the Sovereign Bank account of "Rupok Bhowmik" to checking accounts belonging to two companies named Golu Construction and New Eclipse that are believed to be controlled by the defendants MOHAMMAD CHOWDHURY and/or FAROOQ AHMAD. Bank account records show that Golu

Construction is a likely shell company and its purported address is a mailbox shared by other shell companies in this fraudulent scheme. Checks from the bank accounts of both Golu Construction and New Eclipse were deposited into two accounts belonging to CHOWDHURY's mother-in-law in 2008. CHOWDHURY also wrote large checks from his bank account to his mother-in-law's account in this timeframe. One of these checks was in the amount of approximately \$12,000. As discussed below, a review of CHOWDHURY's 2008 federal tax returns reveals no reported income supporting these disbursements.

CHOWDHURY's mother-in-law then wrote checks from her accounts of approximately \$73,000 and \$95,000 to fund a \$168,000 down payment for the purchase of 85-15 Kendrick Place. The checks written by Golu Construction, New Eclipse and CHOWDHURY, as well as cash deposits, represented nearly all of the funds used to finance the down payment.

26. In 2012, the home at 85-15 Kendrick Place, owned by the defendant MOHAMMAD CHOWDHURY's in-laws, became the subject of foreclosure proceedings. From approximately June 2013 through October 2014, another of CHOWDHURY's mother-in-law's checking accounts at TD Bank received approximately \$100,000 in cash deposits. CHOWDHURY's mother-in-law then made payments of over \$105,000 to service the mortgage on 85-15 Kendrick Place.

27. On September 9, 2015, Magistrate Judge Cheryl L. Pollak of the United States District Court for the Eastern District of New York signed an ex parte application for tax return information covering the years 2008-2014 pertaining to the defendants MOHAMMAD CHOWDHURY, FAROOQ AHMAD and others connected with this fraudulent scheme. (15-MISC-1724). CHOWDHURY and his wife jointly filed federal tax returns on Forms 1040 and/or 1040A for the years 2008-2014. In each of those years, with the exception of 2011 and

2012 for which the Internal Revenue Service has reported no record of a filed return, CHOWDHURY and his wife jointly reported \$0 in wages, salaries, tips, and other income. CHOWDHURY's in-laws filed their returns jointly also for most years between 2008 and 2014 and, in any given year, reported between approximately \$7,500 and \$18,000 in wages, salaries, tips and other income. Thus, neither CHOWDHURY nor his in-laws appear to have legitimate sources of income sufficient to fund the purchase of 85-15 Kendrick Place or to continue to service the mortgage on the property.

28. The investigation thus far has determined that the defendants MOHAMMAD CHOWDHURY's and FAROOQ AHMAD's check-kiting and line of credit fraud activity has resulted in over \$290,000 in losses to various financial institutions. Their credit card fraud activity, including the activity with collusive merchants and shell companies that is described in further detail below, has resulted in losses over \$1 million.

**JAMSHED AND UZMA BABAR'S FRAUDULENT ACTIVITY AS
COLLUSIVE MERCHANTS**

29. The defendant UZMA BABAR is the owner of Isha Grocery and Halal Meat, also known as Grocery and Halal Meat, a sole proprietorship located at 3078 Coney Island Avenue, Brooklyn, New York 11235 ("Isha Grocery"), along with several other related companies apparently located at the same physical address. The defendant JAMSHED BABAR operates the business with UZMA BABAR and is listed as a point of contact on, among other things, applications to credit card processing firms.

30. As discussed below, the Task Force has obtained evidence that the defendants JAMSHED BABAR and UZMA BABAR, as owners and operators of Isha Grocery, have conspired with, among others, the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD, and effected hundreds of transactions involving counterfeit or unauthorized access

devices by, among other things, swiping fraudulent and fraudulently-obtained credit cards at Isha Grocery. The evidence obtained indicates that JAMSHED BABAR and UZMA BABAR, as owners and operators of Isha Grocery, have served as collusive merchants who have facilitated the commission of credit card fraud by, among others, CHOWDHURY and AHMAD.

31. The following examples illustrate the defendants JAMSHED BABAR's and UZMA BABAR's participation in the conspiracy to commit access device fraud using four of the synthetic identities controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD: "Zafar Khan," "Mujeed Khan," the aforementioned "Abigail Singh" and "Anzal Nayar."

32. "Zafar Khan" opened a checking account and line of credit account at Santander Bank in 2012 using the address 85-15 Kendrick Place, Jamaica, New York 11432—the defendant MOHAMMAD CHOWDHURY's residence. "Zafar Khan" has been identified as a synthetic identity because the personal identifying information provided to open his or her accounts does not correspond to a real person. On or about February 21, 2013, March 28, 2013, and April 1, 2013, four advances were made from the line of credit account to the checking account that totaled approximately \$9,800. Between approximately February 21, 2013 and April 2, 2013, "Zafar Khan" made approximately 18 cash withdrawals at Santander Bank branches in Brooklyn and Queens, New York. Sixteen of the withdrawals were for \$500 each and two were for \$400 each. On four dates in that time span, "Zafar Khan" made multiple withdrawals on the same day at different Santander Bank branches. For example, on March 4, 2013, "Zafar Khan" made a withdrawal of \$500 at a Brooklyn bank branch and a withdrawal of \$400 at a bank branch in Howard Beach, New York. On April 1, 2013, "Zafar Khan" made six

withdrawals of \$500 each from bank branches in Brooklyn and two more withdrawals on April 2, 2013.

33. Santander Bank ATM surveillance photos captured the defendant MOHAMMAD CHOWDHURY conducting one of the transactions as “Zafar Khan” on or about April 2, 2013. Overall, either CHOWDHURY or the defendant FAROOQ AHMAD appears on ATM surveillance photos conducting transactions on the accounts of “Zafar Khan” on nine dates between approximately February 21, 2013 and April 2, 2013. Payments made to the line of credit account to repay the advances were all reversed, resulting in a loss to Santander Bank of approximately \$9,778.

34. “Zafar Khan” also opened a credit card at Discover Bank in early 2013 using the same personal identifying information. In March 2013—the time period during which the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD were captured on surveillance photos conducting transactions on the aforementioned Santander Bank accounts—“Zafar Khan” made approximately \$32,460 in charges on his or her Discover Bank credit card. “Zafar Khan” made approximately \$32,418 in payments to the Discover Bank credit card account. All were reversed, resulting in a loss of approximately \$32,460 to Discover Bank.

35. “Zafar Khan” also made multiple purchases at Isha Grocery in the same time span that the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD were conducting transactions on the Santander Bank accounts in the name of “Zafar Khan.” These credit card purchases include \$2,720 on March 4, 2013; \$1,520 on March 9, 2013; and \$2,952 on March 11, 2013. The March 4, 2013 date is but one example of the strong evidence establishing that CHOWDHURY and AHMAD, as “Zafar Khan,” made fraudulent credit card

purchases at Isha Grocery. On that date, “Zafar Khan” made a purchase at Isha Grocery and, as described above, made two withdrawals from Santander Bank branches in Brooklyn and Howard Beach, New York. ATM surveillance photos captured AHMAD conducting the transaction at the Brooklyn branch on March 4, 2013.

36. “Mujeed Khan” also opened a checking account and a savings account at Santander Bank in 2012. “Mujeed Khan” has been identified as a synthetic identity because the personal identifying information used to open his or her accounts does not correspond to a real person. From approximately March 25, 2013 through April 1, 2013, over 17 deposits totaling approximately \$44,100 were made into both accounts, including multiple deposits on multiple dates. Most of these deposits were in the form of checks that were subsequently returned when they did not clear. Between these dates, “Mujeed Khan” made over two dozen cash withdrawals or debit card purchases. On every day between March 26, 2013 and April 3, 2015 (with two exceptions), “Mujeed Khan” made multiple withdrawals of \$500 or more on the same day at Santander Bank branches in Brooklyn and Garden City, New York. On or about April 1, 2013, for example, “Mujeed Khan” made approximately 10 cash withdrawals or debit card purchases. ATM surveillance photos captured the defendant FAROOQ AHMAD conducting transactions on the accounts of “Mujeed Khan” on multiple dates between approximately March 26, 2013 and April 3, 2015. Because the bulk of the deposits to the account were fraudulent, Santander Bank experienced a loss of over \$23,000.

37. “Mujeed Khan” made numerous debit card purchases at Isha Grocery in the same time frame. Among the separate debit card purchases made by “Mujeed Khan” were the following at Isha Grocery: \$2,993 on April 1, 2013; \$2,350 again on April 1, 2013; \$1,020 again on April 1, 2013; \$2,980 on April 2, 2013; and \$1,645 on April 4, 2013.

38. In the same time frame, “Mujeed Khan” also possessed at least three credit cards accounts from Barclays Bank, Citibank and Discover Bank. Between March 5, 2013 and March 23, 2013, “Mujeed Khan” made nearly \$40,000 in credit card purchases in approximately 12 transactions at Isha Grocery. These purchases included two on the Citibank credit card on or about March 8, 2013 for an approximate total of \$3,400, two on both the Citibank and Discover Bank credit cards on or about March 10, 2013 for an approximate total of \$6,300, and two on the Discover Bank credit card on or about March 22, 2013 for an approximate total of \$6,300. Payments made to the credit card accounts of “Mujeed Khan” were reversed, resulting in substantial losses to Barclays Bank, Citibank and Discover Bank.

39. “Abigail Singh” opened a Chase Bank credit card in mid-2012 using the same personal identifying information as that used to open the checking account at Santander Bank discussed above. “Abigail Singh” also possessed credit cards at Citibank, Discover Bank and Barclays Bank. Between approximately June 12, 2014 and July 16, 2014, “Abigail Singh” made over a dozen credit card purchases at Isha Grocery totaling over \$40,000. Many of these purchases came on consecutive days or multiple purchases were made on the same day. For example, “Abigail Singh” made purchases at Isha Grocery on or about June 17, 2014 for \$2,910, on or about June 18, 2014 for \$2,882, on or about June 19, 2014 for \$2,912, and on or about June 20, 2014 for \$2,790. To take another example, on or about July 10, 2014, “Abigail Singh” made two credit card purchases at Isha Grocery for \$2,636 and \$4,860, respectively. And, on or about July 11, 2014, “Abigail Singh” made two purchases at Isha Grocery of \$2,870 and \$4,626, respectively.

40. “Abigail Singh” consistently failed to pay his or her credit card bills and his or her credit card accounts were eventually closed in 2015 for failure to pay and suspected fraudulent activity, resulting in substantial losses to the credit card issuers.

41. “Anzal Nayar” is yet another synthetic identity whose personal identifying information does not correspond to a real person and who was controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD. “Anzal Nayar” opened a Santander Bank checking account in late 2014. In July 2015, “Anzal Nayar” deposited into the Santander Bank account five checks that he or she purportedly wrote to him or herself from a First Interstate Bank account. All of these checks were fraudulent. However, before these checks were discovered to be fraudulent, “Anzal Nayar” made five cash withdrawals totaling approximately \$2,300. Surveillance photos from Santander Bank ATMs captured AHMAD making one of the withdrawals from the “Anzal Nayar” account in July 2015.

42. “Anzal Nayar” also possessed a Chase Bank credit card account. In or around June and July 2015, “Anzal Nayar” submitted checks totaling tens of thousands of dollars to Chase Bank, thereby artificially increasing the credit limit on the account. In the same timeframe, “Anzal Nayar” made almost \$30,000 in credit card purchases. Nearly all of these purchases were eventually reversed, resulting in substantial losses to Chase. Among these purchases were a \$1,900 charge to Isha Grocery on or about July 2, 2015 and a \$1,786 charge to Isha Grocery on or about July 8, 2015.

43. A review of documents has revealed that the transactions at Isha Grocery involving “Zafar Khan,” “Mujeed Khan,” “Abigail Singh” and “Anzal Nayar” are but some of numerous fraudulent credit card transactions effected by the defendants JAMSHED BABAR and UZMA BABAR as owners and operators of Isha Grocery. On about 14 dates from approximately 2013 to 2014, three or more transactions were conducted at Isha Grocery on the same day using fraudulent credit cards controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD and obtained in the names of synthetic identities.

44. From approximately 2012 to 2015, fraudulent credit cards controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD were used to make over \$300,000 in charges to Isha Grocery, with over one hundred transactions using cards with the names of synthetic identities. In March 2013, for example, an approximate total of \$156,237 was deposited into Isha Grocery's known business accounts, and approximately \$88,712 (56%) of those deposits came from fraudulent credit card transactions with cards controlled by CHOWDHURY and AHMAD.

45. The evidence obtained thus far indicates that the defendants JAMSHED BABAR and UZMA BABAR have directly profited from their activity as collusive merchants. In 2011, Isha Grocery maintained the aforementioned Bank of America business account, over which UZMA BABAR has sole authority. During 2011, over \$500,000 in deposits were made to this Bank of America account, primarily from credit card proceeds. Also, in 2013, Isha Grocery maintained a business bank account at Chase Bank. In March 2013, 38 deposits were made to this account that related to credit card proceeds that totaled approximately \$98,500. During this month, 63 cash withdrawals were made from Isha Grocery's Chase account totaling approximately \$53,000. Records reveal that UZMA BABAR signed for at least three large withdrawals totaling approximately \$21,000. In addition, a check written from Isha Grocery's Chase Bank business account to JAMSHED BABAR for approximately \$15,000 was deposited to JAMSHED BABAR's personal checking account at Chase Bank on or about March 14, 2013. This was the only deposit made into this particular Chase Bank account in JAMSHED BABAR's own name. Between approximately March 14, 2013 and April 15, 2013, JAMSHED BABAR made 15 withdrawals via ATM machines and teller transactions from his

personal Chase Bank account totaling approximately \$12,000. The account was subsequently closed in June 2013.

46. The Task Force has uncovered strong evidence that the defendants JAMSHED BABAR's and UZMA BABAR's participation in access device fraud extends beyond the defendants MOHAMMAD CHOWDHURY's and FAROOQ AHMAD's participation in the scheme. For example, a review of Chase Bank records from January 2014 through August 2015 revealed approximately 60 fraudulent credit cards accepted by Isha Grocery in transactions totaling approximately \$140,000. Approximately 44 of those Chase Bank cards, charging an approximate total of \$95,000, are not believed at this time to be controlled by CHOWDHURY and AHMAD.

47. The defendants JAMSHED BABAR and UZMA BABAR have engaged in behavior that, in my training and experience, is strong evidence of knowledge of the fraudulent activity and an intent to conceal it. In or around 2013, for example, JAMSHED BABAR and UZMA BABAR submitted an application for Isha Grocery to Global Payments, a credit card processor. This application included a copy of a 2011 federal tax return showing that JAMSHED BABAR and UZMA BABAR are married, that Isha Grocery is a sole proprietorship and reporting that Isha Grocery's gross receipts were approximately only \$41,500. As described above, over \$500,000 in deposits were made to Isha Grocery's Bank of America account in 2011, primarily from credit card proceeds, much of which was related to fraudulent credit cards.

48. The investigation thus far has determined that the defendants JAMSHED BABAR's and UZMA BABAR's activity as collusive merchants effecting transactions with

counterfeit or unauthorized access devices has resulted in over \$680,000 in losses to various financial institutions.

JASON WALKER AND AHMED SOYBAL

49. From approximately 2011 through 2013, the defendants JASON WALKER and AHMED SOYBAL, also known as “Ali Aloub,” both were salesmen or middlemen who recruited merchants and assisted them in filling out applications with credit card processors and issuers to gain the ability to accept credit cards.

I. AHMED SOYBAL

50. Until September 2013, the defendant AHMED SOYBAL worked as a salesman for AMS Services, a firm in Valley Stream, New York, that provided, among other things, technical services to merchants seeking to accept credit cards. As discussed below, SOYBAL prepared several merchant applications for companies that investigators later determined to be shell companies with no legitimate business purpose. As described in further detail below, these shell companies both received thousands of dollars in purchases from fraudulent credit cards controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD and participated in the check-kiting and line of credit frauds by writing checks, which later bounced, to several of the synthetic identities controlled by CHOWDHURY and AHMAD. As discussed below, from approximately 2011 through 2013, the defendant JASON WALKER owned and operated Merchant Equipment Resources, a firm that provided, among other things, technical services to merchants seeking to accept credit cards. In this capacity, WALKER also prepared several merchant applications for companies that investigators later determined to be shell companies tied to CHOWDHURY and AHMAD.

Merchant Equipment Resources also received seven payments totaling over \$22,000 from fraudulent credit cards controlled by CHOWDHURY and AHMAD.

51. A review of documents revealed that credit cards in the name of the aforementioned synthetic identity “Farhunz Chowdhury” were used on or about January 18, 2013 and January 21, 2013 to purchase or lease numerous countertop credit card swiping machines and pinpad devices at Northern Leasing, a company specializing in the provision of this credit card equipment to merchants. The two charges made by “Farhunz Chowdry” were for \$2,245 and \$160, respectively. Northern Leasing identified the defendant AHMED SOYBAL as the individual who used the cards in the name of “Farhunz Chowdry” to make the purchases. Northern Leasing also identified the defendants JASON WALKER and SOYBAL as salesmen or middlemen who were regular customers of Northern Leasing.

52. While working at AMS Services, the defendant AHMED SOYBAL prepared multiple merchant applications for firms later identified to be shell companies. On or about April 25, 2012, SOYBAL prepared a merchant application for the aforementioned shell company Didarul Home Improvement using 194-18 Northern Blvd., Flushing, New York as the address, which is also used as the address for various synthetic identities and shell companies in the fraudulent scheme. A review of records has revealed that between approximately November 2, 2012 and March 21, 2013, Didarul Home Improvement accepted over 20 credit card transactions from credit cards in the names of synthetic identities controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD. These synthetic identities included the aforementioned “Zafar Khan,” who made two purchases with a Discover Bank credit card on or about March 20, 2013 for approximately \$485 and \$2,493; “Farhunz Chowdry,” who made a purchase with an FIA credit card on or about January 1, 2013 for

approximately \$2,456; “Fairuz Chatterjee,” who made purchases with Discover Bank and Nordstrom’s credit cards on or about January 5, 2013 and January 8, 2013 for nearly \$2,500 each; and “Mark Sydney” who made purchases with Barclays Bank and Citibank credit cards on or about January 10, 2013 and January 19, 2013 for over \$2,000 each. In sum, between approximately November 2, 2012 and March 21, 2013, Didarul Home Improvement accepted charges from credit cards in the names of synthetic identities controlled by CHOWDHURY and AHMAD totaling over \$43,000.

53. The defendant AHMED SOYBAL prepared a merchant application for an entity called Corporate Chef, also known as Midtown Corpcchef, in early December 2012. A review of financial records for this entity demonstrates that it has little or no legitimate business income or expenses. For example, the place of business listed on the application, 176-25 Union Turnpike, Fresh Meadows, New York, is a United Parcel Service (“UPS”) store location with mailing boxes where no business activity is conducted and which is used by other shell companies in this scheme.

54. Between approximately December 23, 2012 and April 30, 2013, Corporate Chef accepted dozens of fraudulent credit card transactions from cards controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD. The transactions included purchases by “Fairuz Chatterjee” with a Discover Bank credit card on or about January 8, 2013 for approximately \$1,436, and “Mark Sydney” with Barclay’s Bank and Citibank credit cards on or about January 11, 2013 for approximately \$1,978 and on or about January 19, 2013 for approximately \$1,406. These transactions are but a few of the dozens accepted by Corporate Chef. Financial records indicate that this shell company accepted over \$100,000 in fraudulent credit card purchases from CHOWDHURY and AHMAD.

55. The defendant AHMED SOYBAL also prepared a merchant application for a company called Premier Catering on or about October 13, 2012. A review of financial records for this company demonstrates that it has no legitimate business income or expenses. For example, its registered place of business, 4506 Queens Blvd., Ste. 303, Queens, New York, is a UPS store location with mailing boxes where no business activity is conducted.

56. Between approximately December 3, 2012 and January 30, 2013, Premier Catering accepted 14 transactions totaling over \$35,000 from cards in the names of synthetic identities controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD. These purchases include those by "Fairuz Chatterjee" with a Nordstrom's credit card on or about January 4, 2013 for approximately \$2,756; "Farhunz Chowdry" with a Discover Bank credit card on or about January 10, 2013 for approximately \$2,486 and with an FIA credit card on or about January 16, 2013 for approximately \$4,799; and "Mark Sydney" with a Nordstrom's credit card on or about January 3, 2013 for approximately \$2,896 and with a Citibank credit card on or about January 30, 2013 for approximately \$2,854.

II. JASON WALKER

57. The defendant AHMED SOYBAL also prepared a merchant application for an entity called Merchant Equipment Resources on or about October 14, 2011. A review of New York State Department of State records for Merchant Equipment Resources revealed that it was incorporated in New York on or about September 28, 2011 and dissolved on or about October 25, 2013. The Certificate of Dissolution lists the defendant JASON WALKER as Vice President. On the signature card of a Chase Bank account for Merchant Equipment Resources that was opened on or about October 8, 2011, however, WALKER is listed as the president of the company. Although WALKER appears to be the owner and operator of

Merchant Equipment Resources, the application prepared by SOYBAL lists another individual named Mosharroff Hossain as the manager of Merchant Equipment Resources.

58. A review of records obtained from Cynergy Data, a credit card processing company, revealed that the defendant JASON WALKER, through Merchant Equipment Resources, prepared four applications between approximately April 10, 2012 and October 25, 2012 for companies later identified as shell companies that accepted fraudulent credit card charges from credit cards controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD.

59. On or about April 10, 2012, the defendant JASON WALKER prepared a merchant application for the aforementioned Corporate Chef. As described above, the defendant AHMED SOYBAL also prepared an application for Corporate Chef on December 11, 2012. Corporate Chef accepted over \$100,000 in fraudulent credit card transactions from cards controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD.

60. On or about April 25, 2012, the defendant JASON WALKER prepared an application for the aforementioned firm Didarul Home Improvement. As described above, the defendant AHMED SOYBAL also prepared an application for Didarul Home Improvement on or about this date. The address used on the application was 114-06 Linden Blvd., South Ozone Park, New York, an address also used by the aforementioned synthetic identities "Fairuz Chatterjee," "Farhunz Chowdry" and "Mark Sydney." The application contains sections entitled "Merchant Site Survey Report: To Be Completed By Sales Representative" and "Further Comments By Inspector" in which the salesman or middleman provides a brief evaluation of the location of the business for which he or she is preparing the application. In this section, WALKER wrote "LOOKS GOOD." As described above, Didarul Home

Improvement's purported business location is a two-family residence in South Ozone Park, New York where no apparent business activity is conducted, and Didarul Home Improvement accepted over \$43,000 in fraudulent credit card transactions from credit cards controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD.

61. On or about October 25, 2012, the defendant JASON WALKER prepared two applications for Premier Catering. In the evaluation sections, WALKER again wrote "LOOKS GOOD." As described above, Premier Catering's purported business address is a UPS store where no apparent business activity is conducted, and Premier Catering accepted over \$35,000 in fraudulent credit card transactions from cards controlled by the defendants MOHAMMAD CHOWDHURY and FAROOQ AHMAD.

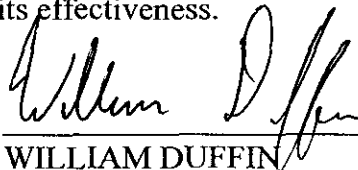
62. In addition to preparing merchant applications for shell companies at the core of the defendants MOHAMMAD CHOWDHURY's and FAROOQ AHMAD's fraudulent schemes, Merchant Equipment Resources, a company controlled by the defendant JASON WALKER, itself received seven payments between approximately January 9, 2013 and March 19, 2013 that totaled over \$22,000 from fraudulent credit cards controlled by CHOWDHURY and AHMAD. These credit card transactions included those by "Zafar Khan" with a Discover Bank credit card on or about March 12, 2013 for \$2,940, and "Mark Sydney" with a Discover Bank credit card on or about January 19, 2013 for approximately \$1,908.

CONCLUSION

WHEREFORE, your deponent respectfully requests that the defendants MOHAMMAD CHOWDHURY, FAROOQ AHMAD, JAMSHED BABAR, UZMA BABAR, JASON WALKER and AHMED SOYBAL, also known as "Ali Aloub," be dealt with according to law.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application for a search warrant. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application for a search warrant. I believe that sealing this document is necessary to preserve the integrity of this ongoing criminal investigation. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and arrest warrants via the Internet, and disseminate them to other criminals as they deem appropriate. Premature disclosure of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.



WILLIAM DUFFIN
Special Agent
Department of Homeland Security
Homeland Security Investigations
El Dorado Financial Crimes Task Force

Sworn to before me this
23rd day of November, 2015


THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK